

Published and Copyright (c) 1999 - 2008  
All Rights Reserved

Atari Online News, Etc.  
A-ONE Online Magazine  
Dana P. Jacobson, Publisher/Managing Editor  
Joseph Mirando, Managing Editor  
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor  
Joe Mirando -- "People Are Talking"  
Michael Burkley -- "Unabashed Atariophile"  
Albert Dayes -- "CC: Classic Chips"  
Rob Mahlert -- Web site  
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Henk Robbers

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,  
log on to our website at: [www.atarinews.org](http://www.atarinews.org)  
and click on "Subscriptions".  
OR subscribe to A-ONE by sending a message to: [dpj@atarinews.org](mailto:dpj@atarinews.org)  
and your address will be added to the distribution list.  
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE  
Please make sure that you include the same address that you used to  
subscribe from.

To download A-ONE, set your browser bookmarks to one of the  
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>  
Now available:  
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!  
<http://forums.delphiforums.com/atari/>

=~::~~::~=

~ Mac Pirates Get Trojan! ~ People Are Talking! ~ AHCC Is Released!  
~ Google's Wildcard Watch ~ Click Fraud Hits High! ~ IE8 Milestone!  
~ Hacker To Get An Appeal ~ Win 7 Beta Extension! ~ ICANN on Fast Flux

~ London Mayor Ribs Obama ~ Western Digital 2TB HD ~ Spam Surges Again!

-\* Wikipedia To Limit User Edits \*-  
-\* Hackers Lurking in Obama's Web Site \*-  
-\* AVG Sees Alarming Rise in Transient Threats \*-

=~==~==

->From the Editor's Keyboard  
"~~~~~"

"Saying it like it is!"

Another week, another snowstorm!! This is really getting to the point of ridiculous. And guess what, another one on the way next week!! And the cold! There are only so many layers of clothing one can wear to stay warm! And to think, our neighborhood was scheduled for an electrical shutdown today in order to switch over lines from some old telephone poles to some new ones that were placed after a local road was widened. Funny, it was too cold for them to do the work so that will get rescheduled.

So, last week I mentioned some of the stupidity related to spam e-mail. It just continues to flow every day, and the subject lines are hilarious, when you can understand them. Really, what is the purpose of spam? I really don't understand the rationale behind most of it. Sure, some of it is an effort to get people to purchase worthless products. Or, an effort to somehow pick up a virus or some other malware. But how stupid do these spammers think most people are? Well, I guess there are some gullible people out there. Or, the spammers just really enjoy behaving like a nasty itch that won't go away! Personally, I'll just keep at them with my trusty delete key.

Until next time...

=~==~==

AHCC Released

LS

Finally, after many years of intermittently hard work and letting myself be distracted by the many beautiful things in a world that is not entirely made up/out by/of computers, AHCC has reached a usable state.

AHCC is a replacement for the renown but proprietary Pur C compiler. AHCC is binary and almost source compatible to Pure C.

You can download AHCC from my homepage (in sig).

The version number is 3.b1

3 after Sozobon v2, b1: the first beta release.  
The language version is C89.

Please, please, before you go fiddling, read the hypertext  
in it's entirety first.

If things are unclear or if you think the hypertext is too  
concise or incomplete, send me a mail.

Have fun.

--

Groeten; Regards.

Henk Robbers. <http://members.chello.nl/h.robbers>

Interactive disassembler: TT-Digger; <http://digger.atari.org>

A Home Cooked C compiler: AHCC

=~::~~::~~::~=

PEOPLE ARE TALKING  
compiled by Joe Mirando  
[joe@atarinews.org](mailto:joe@atarinews.org)

Hidi ho friends and neighbors. Well, another week has come and gone, and  
we've got a few more UseNet messages to work with, so we'll have at  
least something Atari-related to talk about this week! Yea!

But before we do, there are just a few things I want to mention... all  
of them dealing with <sigh> politics.

Now, I really hate to categorize people. Even those who categorize  
themselves... Republicans, for instance. You'd think that, despite the  
fact that you call yourself a Republican, you'd find times when you just  
had to agree with the other guy because you could see the value and  
wisdom of what he was doing.

I guess not, huh? This past week, when the President's stimulus package  
came up for a vote, not a single Republican voted for it. Not one.

Could it possibly be that they really believe that it's the wrong  
combination of the wrong things at the wrong time for the wrong price?  
It's possible, of course, but ALL of them? I don't think so.

Could it be that the leadership of the Republican party is pushing them  
to vote the party line and against the President's package? Again, it's  
possible, but I don't think that, in and of itself, that'd be enough to  
get every Republican member of Congress to vote against it.

I think it's more likely that the Republican members of Congress are  
doing what they do best... watching out for themselves.

Let's face it, after the whoopin' they took this last election, the only  
Republicans left in Congress are from very, very conservative districts.  
And members of the house are up for election every two years. That  
means, in campaign terms, that they've got only a handful of months left

before they've got to start campaigning again. As a Republican in a very conservative district, you're going to have to tow the line on every single vote and give your stick-in-the-mud, stuck-in-the-cold-war constituents exactly what they want... opposition to everything the Democrats want to do in every way possible... or you'll find yourself out in the cold with some greasy, pseudo-conservative yes-man being put up against you by your own party.

Of course, they're hobbled by the fact that they don't have the numbers in either the House or the Senate to do any real damage, but they're gathering capital every time they vote against a democratic measure with their voters and, they hope, strengthening their chances of taking back some seats in the next election.

This is what I've been saying for the past several years... that they were going to throw the '08 Presidential election and concentrate on taking back what they could of the House and Senate in '10.

The whole situation reminds me of an episode of one of my favorite television shows: The West Wing. The minority party was complaining, just as the Republicans are now, that they're being "shut out" of law making and major decisions. The President's Chief of Staff, Leo McGary (played by John Spencer) looked at the staffer who mentioned it in disbelief and said, "We won the election. That means the other guys can take a seat and shut up for four years."

Does that sound familiar? The President said pretty much the same thing to the Republican leadership when they "presented" their plans to him... like he was going to bend over backward for them after these guys bent us all over forward for the last eight years. Boner, sit down and shuddup.

Now, you're going to hear the Republicans whine at every turn about being 'shut out' of decision making, and that they're not getting a chance to contribute. The problem with that is that it's a lie. The President has reached 'across the aisle' more times in the last month (of which he's been President for only 2 weeks) than the former White House resident did in his entire two stolen terms. Remember "The Uniter"?

Since the Republicans were 'in power' for the majority of those eight years, they felt entitled to dictate terms. Now that they're the minority (and a very minor minority at that), they feel that they are entitled to... wait for it... dictate terms! Hell, Ronnie Reagan ain't dead! He just crawled up into John Boehner's colon.

Now, if these guys were so all-fired worried about the economy and the plight of the middle class and the real, tax-payin' Americans, it seems to me that they would have done something a long time ago when many people saw this coming.

Well, the fact is that they DID do things... they circled their wagons, they grabbed for all the wealth they could and "got while the gettin' was good". They're now talking about cutting taxes, and while that sounds good, it's never as much as a stimulus as you'd think. Because while everyone likes the idea of paying less tax, we also like the idea of decent roads, a good education for our kids, social services and all the "good stuff" that filters down... A decent amount of money makes its way to your local government from the state. A descent amount of the state's money comes from the federal government. And where does the

federal government get its money? Anyone? Anybody at all? You... you in the back.. c'mon just shout it out if you know it... that's right...from taxes! You get a gold star.

Now, right next to cutting taxes, in their tiny little hearts is cutting spending. Hey, everyone's against waste in government, right? Okay. Let's cut some waste... farm subsidies... I'm not a farmer, so what do I care? Ask me again next year when we're paying triple for meat and double for milk.

Let's cut the education budget. That'll cut your taxes for sure. Well, no it won't, actually. Education is the most underfunded aspect of government funding there is. What you don't pay for education now is going to end up costing you big-time in just a few years. And don't even get me started on vouchers. You can stick all those vouchers with Ronnie Reagan and light 'em with a match. Instead of bailing out on the public school system, we need to be supporting it. The reason our state colleges are having to raise fees and tuition the way they are is because we've gotten accustomed to being cheap about it and now we're having to pay for it double out of the other pocket.

There's an email going around right now that draws a parallel between pig farming and socialism... I know, I don't particularly think it's a good analogy my self, but Karl Rove probably thought it was a good pairing. Anyway, the meat and potatoes of the email is that we're headed for socialism and all its evil connotations.

But the plain and simple fact is that the Democrats aren't pushing us toward socialism. The Republicans are pushing us toward fascism.

Socialism is when the government takes care of every facet of your life... the Democrats' most workable plan for healthcare (and could anyone but these Republican toads have you stand an cheer AGAINST healthcare like it was Ho Chi Min's personal embrace?) entails telling insurance companies and employers how they have to treat the rest of us.

Fascism, on the other hand, is the government using a three-prong fork to push us into doing what it wants... First comes the of instilling fear in the populace, telling them that they need to relinquish certain rights in order to remain safe. Next prong: Make everybody else in the world the bad guy. We're entitled to break whatever rules we want to because we're the good guys now. Prong three is giving special consideration to the corporations. After all, if the corporations don't do well, they'll surely never be able to afford to let us make a living, so we have to let them suck the life-blood out of us or we're unpatriotic. Look around. The past eight years have been a study in modifying the American psyche to accept a fascist bent. Like it or not, believe it or not, that's what they've been up to. That's the only way all the lies and deceit and maneuvering make sense.

And while I'm thinking of it, do you remember the days when all you needed was a high school education and a willingness to work to be able to support a family? A 40-hour-a-week job that you could leave behind at five o'clock and you'd be able to buy a nice little house and a new car every five or six years and raise your family without worrying about every little thing? Yeah, I remember it too...

But the most amazing thing to me... the most brain-busting thing of all the brain-busting things this crew of airport-restroom-lurking, two-mistress-having, seein'-russia-from-your-state caricature is that

pain-killer-addicted, immigrant-employee-pressuring gasbag, Rush Limbaugh this week.

It seems that Mr. Do-As-I-Say-Not-As-I-Do is so patriotic... that he loves this country so much... that he's hoping that the new President fails. Now class, what happens if the President fails? Anyone? You in the back? That's right... we all fail. Mr. Mealy-Mouth loves this country so much that he's willing to see it go down the tubes to prove his feeble little point. Yep. That thar boy be a patriot.

Well, to quote Forest Gump, that's about all I have to say about that.

Before we get into the UseNet stuff, I want to leave you with this little brain buster...

I can tell you who your favorite author is, and I thank you in advance for it!

Just follow along....

- 1) Pick your favorite number between 1-9
- 2) Multiply by 3
- 3) Add 3, then Multiply by 3 again(I'll wait while you get the calculator . . . )
- 4) You'll get a 2 or 3 digit number . . .
- 5) Add the digits together

Now with that number see who your favorite author is from the list below:

1. John Grisham
2. Dan Brown
3. Robert Louis Stevenson
4. Mark Twain
5. Arthur C. Clarke
6. John Updike
7. Ernest Hemingway
8. Stephen King
9. Joe Miranda
10. Rudyard Kipling

Go ahead try it again. I dare you. Oh, and thank you for your support!  
[Grin]

Now, if you were able to do the math without a calculator, thank not only a teacher, but the system that provided the teacher. If you had to use a calculator, thank the teachers that taught the guys who design calculators, and get back to your fry-o-lator.

Let's get to the news, hints, tips and info available from the UseNet.

From the comp.sys.atari.st NewsGroup  
=====

Henk Robbers posts this about his C compiler:

"Finally, after many years of intermittently hard work and letting myself be distracted by the many beautiful things in a world that is not entirely made up/out by/of computers, AHCC has reached a usable state.

AHCC is a replacement for the renown but proprietary Pure C compiler. AHCC is binary and almost source compatible to Pure C.

You can download AHCC from my homepage (in sig).

The version number is 3.b1  
3 after Sozobon v2, b1: the first beta release.  
The language version is C89.

Please, please, before you go fiddling, read the hypertext in it's entirety first.

If things are unclear or if you think the hypertext is too concise or incomplete, send me a mail. Have fun."

'Phantom' asks about the state of the Atari community:

"[Does] anyone have a rough estimate of how many Atari 16-32 bit owners/users there are in the USA/Canada and OverSeas that are Active with there Computers?

The activity in this NewsGroup suggests that a lot have stopped or moved on.

I know of a couple of friends that are working on some Atari related projects and may release some of the software/hardware if there are enough Users left that may actually pay for shipping costs of a Disk or CD.

Or is there other reasons, why Atari owners/users do not use this newsgroup anymore?

Maybe some of the Atari Dealers that are left can give a number of customers in the past year so we can get a feel of how little of us is left."

'GMAN' tells Phantom:

"I still have my Mega ST, a 520ST, and a MegaSTE 4MB that are all in storage. Have a couple of mono and color monitors including the prized PS3000 model. Just haven't unboxed them in 3 years since I moved into our new home."

Ronald Hall tells Gman:

"Wow, I can't imagine going 3 \*days\* without using my Atari's, let alone 3 years!

I've got my highly modified Falcon, Modded Mega ST that runs my BBS, and now the STacy I'm working on. All of these get -daily- usage. I guess my Mega STe and 800XL get the least use, but they are still used weekly."

GMAN replies:

"I used to use mine everyday, and logged many an hour with BBS's around the country. But after working oh so many years ago at a job repairing PC's at a place called Incredible Universe, the working for Bell and Howell and CompUSA.

I basically moved on. Hard to resist the PC urge when i could get items at coast from many of my places of employment. So now , its a matter of space and time. Back then my wife and I didn't have 3 sons, all getting into the teenage years now. I have way to many consoles and i need to spend my time with the kids and not my game systems or Ataris or PC's now for that matter.

I will brush off the dust soon and relive the fun but i can guarantee now that probably half the disks might not work anymore, and no online usage for me.

If anyone wants some of the stuff from the old Stormbringer BBS, software that is, i can dump it to CD or DVD for a small cost for postage."

Phantom tells Gman:

"I am glad you still have your Atari stuff.

Do you plan on using it in the future, or would you be interested in selling or trading some of your Atari Items?

I could use a good Mono and Color monitor and a MegaSTE. Maybe we could work out some type of deal for some or all of it, if you are interested.

I'd be really interested in the MegaSTe, Does it have a internal Hard Drive? Any upgrade boards in it?

I don't know much about the PS3000, Is that a Color VGA made by Atari?

I am looking for 3rd party hardware and software for the STs-Falcons too. Things like graphics cards, Digitisers, Samplers and odd bits of hardware and software. TOS Upgrades/Switchers, CPU upgrades and Speed boards.

By the way, did you ever have a CDRom drive connected to any of your Ataris?

If you plan on keeping your Ataris, I do have some hardware and software that you might be interested in when you get a system setup.

Do let me know if you are interested in selling/trading some or all of it.

And if there is any Atari Items that you are looking for, I may be able to help you with that. I have a lot of different stuff."

Mark Duckworth adds:

"I'm still active. Over christmas I started to delve into major changes into GEM instant messenger. I really got far and really improved it but I ran into a major roadblock. The libfaim that I use doesn't support the buddy icon server protocol which is required by most clients these days. I've started to make said changes but.. yeah... effort. Though it is basically quiet, still in the planning stages and not definitely or moving (read: extremely vaporware) there is some movement behind coldfire hardware again. I myself have most of what I need to get my coldfire board running. I still need to get an etherneec but it seems nobody is selling them. I also think they're not worth \$75 or whatever people keep wanting to charge for them so I'm thinking about producing my own batch but within the files there are not suitable files to send to a PCB house."

Lonny Pursell adds his thoughts:

"I'm still active, GFA will see more updates. Also IRC chat is active on a daily basis. Plenty of them don't bother with usenet. Why spend time here when you can often get a reply in real time.

I also agree with the comments about forums. Sure usenet is easy to manage from a user point of view on the surface if you can skip the crap and don't go nuts, but the forums do have more control. Spam really don't exist there, so I see why people gravitate to the forums."

Stephen Moss adds his thoughts on the lack of activity on the UseNet:

"In my opinion, the reason there is not much traffic here these days is because people became fed up with the time and cost of dealing with the amount of Spam and Flame wars that regularly appeared here especially when Sinclap posted anything. This resulted in a lot of people moving to forums where such things are easily stopped because...

- a) Requiring an account makes it hard to spam whereas spam bots can easily invade newsgroups.
- b) Threads that descend flame wars of otherwise get out of hand can be locked so that no more posts can be made thus depriving the fire of fuel
- c) The accounts of those who Spam or Flame can be closed and so such people eventually get fed up of having to open new accounts to access the forum and go away.

Ironically most of the reasons above seemed to have declined in proportion to the decline in posts here, presumably they think it is no longer worth the effort but may change there minds when should things pick up.

In addition to this I am sure there are a few who have left the Atari scene and some for who life has got in the way and have not had the time to use their Ataris/post. There is also the odd new addition/returnee to the Atari world but in a time where things like Facebook are prevalent most companies are using forums of them are probably more used to web forums than newsgroup or not old enough to really know what newsgroups are, plus unlike newsgroups you can post/PM someone the file they want

or post an image help explain what you are talking about on a forum.

There are many Atari forums around such as Atari Age ([www.atariage.com](http://www.atariage.com)) which has a regular flow of ST/TT/Falcon post. Jaguar Sector II (<http://www.jaguarsector.com/index.php?>) which as the name suggest is mainly Jaguar orientated, although it does have forums for 16/32 but computer is it less active. Another is Atari Forum (<http://www.atari-forum.com/>) this appear to be purely for all things ST/TT/Falcon, there are probably others but check these out.

Ian McCall asks for help finding an iconic image from years past:

"Does anyone have the example image of a tiger that used to come with the ST, preferably in a modern format such as gif or png? I was surprised that a quick search for "GEM tiger example atari" on Google didn't come up with anything, unless I'm just being dumb this morning."

Martin Byttebier tells Ian:

"I've put that image on my webspace

<http://users.telenet.be/tos4ever/downloads/tijger.jpg> "

Michael Schwingen tells Martin:

"Um - that's not the GEM tiger, that's the standard postscript demo."

Martin replies:

"Ok, thanks.

A kind soul has send me the correct picture and it's now on my personal webspace. <http://users.telenet.be/tos4ever/downloads/tiger-mono.jpg> "

Rodolphe Czuba posts this about SuperVidel:

"[http://nature.atari.org/Pics/SuperVidel\\_prototype\\_rev1.jpg](http://nature.atari.org/Pics/SuperVidel_prototype_rev1.jpg)

Who was not trusting these guys? Now it will be possible to design a new Atari!

Mark Duckworth tells Rodolphe:

"I for one always trusted their intent. But after seeing how long the EtherNAT took I had my doubts... Not that I thought they were criminal or incompetent but it's just a tough thing.

I'm glad to see something real. I've been longing for the supervidel or the CTPCI for a couple years now. Really either solution will give me some hope."

Well folks, that's it for this time around. Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

$$= \sim = \sim = \sim =$$
[illegible]
$$= \sim = \sim = \sim =$$
[illegible]

## Sony Loses \$2.9 Billion, Makes New PSP Colors

What's the best way to recover after a \$2.9 billion annual operating loss? Sony says: introduce new PSP colors!

The PSP-3000 is receiving a carnival makeover in Japan with the introduction of four new retina-melting colors: Radiant Red, Vibrant Blue, Bright Yellow and Spirited Green. The PSP hardware specs remain the same, and the ¥24,800 (\$279) bundle includes a 4GB MemoryStick, a pouch and a hand strap.

These new colors hit the Tokyo streets in March. No word yet on whether these colors will make it over to North America, or if we'll be left out of the party.

Resident Evil 5 Demo Out for Xbox 360 Gold Members Only

Zombie buffs rejoice, Capcom's Resident Evil 5 demo is available now for Xbox 360 "Gold" members in the U.S. Presumably similar to the surprisingly mediocre Japanese demo; it looks like the U.S. version may in fact sport an extra level and a few new weapons.

Here's the salient bit from Capcom's press note:

/As part of the demo launched today, fans will be able to get hands-on with new "Resident Evil 5" features including three new levels of single- and two player co-op play (limited to Gold members), characters, weapons and environments. In this latest installment of the renowned survivor-horror franchise, returning "Resident Evil" hero Chris Redfield is joined by new partner Sheva Alomar to take on the frightening effects of the latest bioterrorist attack in the depths of Africa./

There's a catch: If you want the Resident Evil 5 demo today, you'll have to pay for it. Really. How much? What Microsoft charges for an Xbox Live "Gold" membership - \$50 a year - if you don't already have one. Freebie "Silver" members have to stand at the window looking in until Thursday, January 29th. And PlayStation 3 owners are out of luck until sometime next week.

Which raises the question: Should demos be timed exclusives? It's one way to distance yourself from the competition, sure, all other things being equal in a multiplatform scenario. And it's certainly Capcom's prerogative.

But I'd personally rather see Microsoft and Sony hammer out post-release exclusivity deals, like downloadable content (DLC) only available on one or the other. There's nothing special about the Resident Evil 5 demo, save for its early availability. While time is a commodity, I'm disappointed when it's the only one a company can come up with to tilt the playing field.

I've also made no secret of my disdain for Microsoft's annual Xbox Live membership fee for online multiplayer and matchmaking. It's too bad Microsoft's attempting to distinguish its pay-for "Gold" service from the Xbox 360's default "Silver" by turning a demo (not really "premium" content by itself) and co-op play into a membership drive.

To clarify: I have no beef with annual membership fees, when they're justified. But early demo access and online multiplayer capabilities don't make the grade.

#### NFL Players Get Shot At A Virtual Championship

With just days until Super Bowl Sunday, a who's who of NFL players and celebrities are lined up for one of the hottest parties in Florida on Thursday - the annual videogame competition, the Madden Bowl.

The 15th annual competition pits the best NFL pros in a single-elimination tournament to find out who the best "Madden NFL 09" gamer is on Microsoft's Xbox 360.

"A lot of guys play video games, especially "Madden," and everybody thinks they're good, so Madden Bowl allows players to find out who's the best," said New York Jets' Brad Smith.

"You want to have those bragging rights for the next year."

This year's tournament includes a pair of combatants who will face off on the real gridiron Sunday in the big game - Arizona Cardinals running back Edgerrin James and Pittsburgh Steelers running back Willie Parker.

Other players that will take part in this year's Madden Bowl include Tampa Bay Buccaneers wide receiver Antonio Bryant, Jacksonville Jaguars running back Maurice Jones-Drew, New York Giants defensive end Justin Tuck and Dallas Cowboys linebacker DeMarcus Ware.

EA Sports is introducing a first-ever Madden Bowl XV Rookie Play-In game between quarterbacks Mark Sanchez of the USC Trojans and Matt Stafford

of the Georgia Bulldogs, both of whom have declared for the upcoming NFL Draft.

The winner of this pre-tournament game will take part in the big competition that always take place in the home city of the Super Bowl.

Last year, Baltimore Ravens running back Willis McGahee took home the trophy in Arizona. He faced off against Buffalo Bills running back Marshawn Lynch.

"I didn' even think I would make it past the first round because I' not a "Madden" player like some of these guys," said Lynch. "When I got to the championship game, my first thought was, "Damn, there's somebody out there that's worse than me.""

Microsoft will offer gamers at home the chance to play "Madden NFL 09" against Baltimore Ravens linebacker Ray Lewis via Xbox Live during the festivities.

Attendees will be able to mingle with some of the biggest names in the NFL, including popular wide receivers like Terrell Owens (Dallas Cowboys), Chad Johnson (Cincinnati Bengals) and Reggie Wayne (Indianapolis Colts).

"When Madden Bowl first started, EA had to almost beg people to attend," said Jon Robinson, editor at ESPNVideogames.com.

"Fourteen years later and they're turning people away."

Tom Goedde, vice president of marketing at EA Sports, said the Madden Bowl started coming together as a media event around 2000, when celebrities like P. Diddy and athletes like Joe Montana and Barry Sanders started attending.

Today, satellite trucks line up outside and hundreds of media covering the event and the celebrities attending the bash.

"I think Madden Bowl is designed to show retailers that EA will promote the game heavily, and encourages them to participate by promoting "Madden" throughout the Super Bowl build-up," said Michael Pachter, videogame analyst, Wedbush Morgan Securities.

"A couple years ago we doubled down and partnered with NFL PLAYERS to put on the Rookie Madden Bowl in Los Angeles in May and it's been fun to get the young guys in the mix as well," said Goedde.

Washington Redskins wide receiver Devin Thomas won the last Rookie Madden Bowl in May 2008 in Santa Monica.

"You take a bunch of guys who are competitive on the field and give them videogames and it makes for a great event," said Thomas. "It's something we all love to see."

=~::~~::~=

The Latest in Computer Technology News  
Compiled by: Dana P. Jacobson

Hackers Lurking in Obama's Web Site

U.S. President Barack Obama ran a successful Web 2.0 campaign last year. Now, as president, he's got to deal with a very Web 2.0 problem: hackers abusing the social-networking features of his Web site.

Hackers have registered bogus accounts on Obama's online community, my.barackobama.com, where they are posting images designed to set off a chain of events that lead to malicious Trojan horse programs. These programs are stepping stones used by hackers to download more and more malware onto a victim's computer.

The problem on Obama's Web site is not unique. Hackers and the operators of popular Web sites are often caught in a cat and mouse game, with the bad guys constantly finding a new way of uploading malicious programs just as soon as one avenue of attack is closed. Social-networking sites want to give their users as many cool ways of enhancing their own Web pages as possible - my.barackobama.com lets users create their own blogs - while at the same time reining in any misuse.

"The U.S. Presidential campaign has shown the world how governments can leverage Web 2.0," Websense wrote on a company blog outlining the issue Monday. "However, this ... is yet another opportunity to spread more malicious code."

The scam starts when the victim sees what appears to be a video posted to the my.barackobama.com Web site. It reads simply "click here to see movie." By clicking on the fake video, the user is taken to another Web site that looks like a YouTube page filled with pornography. Clicking on the fake YouTube link prompts the victim to download what appears to be a piece of video decompression software called a codec. The fake codec is actually the Trojan program.

To make matters worse, hackers are also putting links to the malicious Barackobama.com pages in comment forms all over the Web, making them likely to come up as Google searches results. Because of the way search engines work, pages hosted on a popular site like Barackobama.com are typically given a higher search result ranking than other Web pages.

Only about a third of the major antivirus vendors are now detecting this Trojan program, Websense said.

'Obama Worm' Probably A Student Prank

A new Internet worm that displays an image of President Obama is likely a prank by a student, several security experts speculated on Thursday.

Walling Data, a distributor of AVG security software, said the worm it discovered on computers at an Illinois grade school spreads via external devices like USB drives and network shares. Once a week, on Mondays, it

displays a photo of President Obama's face in the lower right corner of screens on infected computers, but otherwise appears to be more of a nuisance than a threat.

The worm looks like a variant of MAL\_OTORUN code that spreads using thumb drives and network shares, said Jamz Yaneza, a senior threat analyst and researcher at Trend Micro.

"Someone played around with one of the many number of DIY malware kits and just added this small social engineering bait of Obama's picture," he wrote in an e-mail. Given that it lacks a malicious payload, "it is probably some prank by a student since today's 'serious' malware, as you may have noticed, would have at least installed a keylogger to steal some information."

Roger Thompson, owner of Thompson Security Labs who said he was informed about the worm from AVG, wrote on his Thompson Cyber Security Labs blog a note to administrators at the school where the worm was found: "There's some chance one of your students wrote it. Find your smartest, geekiest, dweebiest kid, and look hard at him. Remember, the geek shall inherit the earth."

#### Google's Wildcard Watch

Steve Ballmer, who just announced to the troops that Microsoft was firing 5,000 employees due to the recession, might be excused for wanting to slam his head against the wall at this point.

After reporting quarterly earnings, Google finished Friday up more than \$18. So at this point, at least, it's still Google 1, Recession 0. The cool kids have the upper hand - at least for the time being.

I'm the last to suggest that Google is immune to the drag of an economic slowdown. Everyone these days is obviously tightening their belts, and Google is no exception. The company let go of 100 contractors and recently ordered three projects shut down as cost-savings measures. (How long before more money losers get dumped?)

In the meantime, however, Google's advertising business held up remarkably well in the fourth quarter, all things considered. Even though the economy headed south, Google's paid clicks increased 18 percent in the fourth quarter compared with the same period a year earlier.

But if you're a glass-half-empty type, is this a harbinger of trouble? Revenue growth slowed to an 18 percent annual rate, compared with 31 percent in the third quarter. Listening to Eric Schmidt's team handle Wall Street's questions on the company's conference call Thursday afternoon, you realize that the folks running Google are too experienced to believe they can defy history.

At best, they may be able to slow it down through a combination of managing smartly and prudent cost-cutting. Apropos, here's what Google's CFO, Patrick Pichette, had to say:

"I think the management team is really working with two agendas always. One is, manage our resources prudently. I think Eric was right in saying in some ways the easy part was done in Q4. In that sense, this is a

worldwide recession with a lot of visibility about what's going to happen. We just have to be prudent, and therefore, we're focused."

Focused. But that's not the same as arguing the keyword search business is recession-proof. With more businesses and consumers reducing spending, how long before advertisers have to lower their keyword bids?

Business was so bad for so many companies in the fourth quarter that many retailers were offering distress sales in a rush to clear inventory. And that affected search patterns during the last couple of months of 2008. Here's what Jonathan Rosenberg, Google's senior vice president of product management, had to say about the anomaly:

"Interestingly, what we saw in November and December was consumers searching much more disproportionately for two-for-one, for sales, for coupons, and advertisers really trying to make sure that they were able to sell the inventory which they purchased when they were anticipating a better economic situation."

"So, one of the things we have to ask ourselves now is how much of that inventory has actually flowed through the system...Obviously, we would be adversely impacted if there were less total commerce moving forward. So that's really the wildcard from a user standpoint that we need to watch."

He's quite right about that. Nobody knows the sort of hand Google's likely to get dealt. Anybody who tells you otherwise is simply a pumper or a dumper. Or maybe they just work for CNBC.

The rap against Google is that it's just a glorified one-trick pony. When I hear that refrain (usually, from Microsoft folks,) I nod and add, "Yeah...and that's still one helluva pony."

But here's the rub: if advertising comes under more pressure during the next 12 months, does Google have the chops to come up with another big idea to compensate for any financial shortfall? Google's page-ranking technology was a breakthrough and a huge moneymaker. Even Google's biggest fans have acknowledged that nothing remotely similar has since made its way off the drawing board.

And who knows? If stuff like Google Scholar is the best that Google can muster, maybe Ballmer won't have to slam his head for much longer. To be continued...

#### NASA Hacker Wins Right To Appeal Against Extradition

Gary McKinnon, the man accused by U.S. prosecutors of "the biggest military hack of all time," has won the right to a judicial review of a Home Office decision to extradite him to the U.S.

Lord Justice Maurice Kay made the ruling at the High Court in London on Friday. The Home Office had refused to halt the extradition proceedings, despite McKinnon having been diagnosed with Asperger's Syndrome, a condition on the autistic spectrum.

McKinnon's solicitor Karen Todner told ZDNet UK on Friday that she was "very pleased" about the High Court decision.

"It's a step in the right direction," Todner said. "We've got permission for a judicial review, and that shows we have an arguable case."

McKinnon's legal team applied for the review on the grounds that McKinnon's medical condition had not been taken into account by the Home Office or any UK court in deciding his extradition. If convicted by the U.S., McKinnon faces a 70-year sentence in a maximum security prison, his barrister Edward Fitzgerald QC has argued.

Todner said the review was granted on the grounds that the extradition may breach Article 3 of the European Convention on Human Rights, which states that no one shall be subjected to "inhuman or degrading treatment or punishment."

Professor Simon Baron Cohen, the Cambridge University specialist in developmental psychopathology who initially diagnosed McKinnon, said on Tuesday that McKinnon suffered the risk of "psychiatric difficulties" including depression and anxiety should he be extradited and imprisoned.

Home secretary Jacqui Smith turned down McKinnon's second appeal against extradition in October 2008, after the diagnosis of Asperger's syndrome in summer 2008.

The judicial review will not take place until after the director of public prosecutions, Keir Starmer, has decided whether to charge McKinnon. McKinnon sent a signed confession to Starmer in December admitting offenses under Section 2 of the Computer Misuse Act, in the hope of being prosecuted under UK law.

Starmer is due to give his decision in just over two weeks. If he chooses to charge McKinnon, the judicial review will not take place, as extradition proceedings will cease. Otherwise, the judicial review will go ahead "towards the end of March," Todner told ZDNet UK.

#### London Mayor Ribs Obama Over British 'Crank' Hacker

London's mayor called Tuesday on US President Barack Obama to stop efforts to extradite a Briton accused of hacking into the Pentagon, calling it a "last piece of neocon lunacy" from the Bush era.

Boris Johnson said Gary McKinnon, 42, who could face life in prison if extradited and convicted in the United States, is just a "crank" who believes in UFOs and poses no genuine threat to US security.

He also accused British authorities of being "spineless" in not stopping the extradition process.

"It is good news that (Obama) is getting rid of Guantanamo and water-boarding and extraordinary rendition, all the dread apparatus of the Bush regime," he wrote in a column in the Daily Telegraph newspaper.

"But before we all get too misty-eyed about the new era, and before Barack devotes himself entirely to the meltdown of the banks, there is one more thing in his diplomatic in-tray.

"There is one last piece of neocon lunacy that needs to be addressed,

and Mr Obama could sort it out at the stroke of a pen," wrote the colourful former journalist, referring to the Bush era's neo-conservative policies.

McKinnon faces life in jail if convicted by a US court of gaining access to 97 computers in 2001 and 2002, following the September 11, 2001 attacks in the United States.

He says he was looking for evidence of unidentified flying objects (UFOs), while his supporters say he has Asperger's Syndrome -- a form of autism -- and could attempt suicide if he is forced to go to the United States.

"It is a comment on American bullying and British spinelessness that this farce is continuing, because Gary McKinnon is not and never has been any kind of threat to American security," wrote Johnson.

"Mr McKinnon believes in UFOs, and he is one of the large number of people who think that there is a gigantic conspiracy to conceal their existence from the rest of us, and that this conspiracy is organised by the US government."

Johnson, who won City Hall for the opposition conservatives in May, added: "We have a word for people who persist in believing in alien abduction. They are cranks, and they do not deserve to be persecuted."

"It is time for Barack Obama to show the new leadership the world has been crying out for.... In the words of the spiritual with which he began his inauguration ceremony, it is time for the new president to let our people go."

#### Wikipedia Considers Limiting User Edits

Just as Encyclopedia Britannica is moving in the direction of user-based entries, Wikipedia might soon be clamping down on theirs.

Wikipedia is apparently considering instituting a new editorial process that would put better safeguards in place and require all updates to be approved by a "reliable" user. The so-called Flagged Revisions process would allow registered, trusted editors to publish changes to the site immediately. All other edits would be sent to a queue and would not be published until they get approved by one of Wikipedia's trusted team of editors.

The proposal comes in the aftermath of a false entry that was posted by a user, saying Senators Ted Kennedy and Robert Byrd had died after an inaugural luncheon last week.

News.com Poll Encyclopedic reliability Which Web encyclopedia content policing system do you prefer? One that's policed by users (Wikipedia-style) One that's policed by site staff (Britannica-style).

On his public discussion page, Wikipedia founder Jimmy Wales said, "This nonsense would have been 100 percent prevented by Flagged Revisions," adding that the system gives the site the flexibility to cover breaking news stories quickly while avoiding some of the shenanigans it's seen in the past.

The German version of Wikipedia has been using the system for a while now (partially since May and fully since August, according to one Wikipedia user). But Wales himself points out one major problem with the German model, citing delays of up to three weeks before edits get approved and go live.

"Our version should show very minimal delays (less than 1 week, hopefully a lot less)," wrote Wales, "because we will only be using it on a subset of articles, the boundaries of which can be adjusted over time to manage the backlog."

Which subset of articles would be flagged and exactly how those boundaries would be set isn't clear from the discussion.

Wales writes in his comments that 60 percent of users who responded to a poll approved of the move. Think Wikipedia's plans are a bad idea? There's time to give your input. Wales has asked people opposed to the Flagged Revisions plan to propose other workable solutions to the problem of wiki malfeasance.

#### Windows 7 Beta Availability Extended

Microsoft has extended the general availability of the Windows 7 beta until February 10 due to the software's popularity, the company said.

Microsoft was scheduled to remove the beta from the Windows 7 download site this past Saturday, but is allowing people to download it for another few weeks, the company said in a blog post.

People have until February 10 to start the download of the software, but downloads have until February 12 to be completed, according to the post, attributed to Brandon LeBlanc, a Microsoft Windows communication manager. No one will be able to begin downloading the Windows 7 beta after February 10, Microsoft said.

Microsoft made the first beta of Windows 7 available to the general public on January 10, a day later than planned because interest in the beta crashed its Web site when the company first posted it the day before. So far, Windows 7, the follow-up to the disappointing Windows Vista OS that fixes many of problems users reported with Vista, has gotten positive reviews from early users.

Microsoft wants to give people plenty of time to prepare for the end of the beta's public evaluation period, according to LeBlanc's post. On Tuesday, the Windows 7 page will warn users that time is running out to download the software so they can prepare for the Feb. 10 deadline.

However, the new deadline does not apply to MSDN (Microsoft Developer Network) and TechNet subscribers, who will have access to the Windows 7 beta through its entire testing phase, according to LeBlanc.

Additionally, if a user has downloaded Windows 7 but does not have a product key for the software, Microsoft will continue to provide those to beta users indefinitely. A product key validates that a user's copy of the software is legitimate.

## Microsoft Will Fix Problems Before Final Windows 7

Now that a beta version of Windows 7 has been released to the public, Microsoft is letting users know what to expect next. Instead of moving on to a release candidate as in the past, Microsoft will first resolve problems reported by users.

Windows 7 beta was released Jan. 7 at the Consumer Electronics Show to MSDN, TechNet and TechBeta subscribers, and then to the rest of the world shortly thereafter.

"As we have said before, with Windows 7 we chose a slightly different approach which we were clear up front about and are all now experiencing together and out in the open," said Steven Sinofsky, Microsoft's senior vice president for Windows, in a blog post Friday.

Microsoft is working with PC makers, hardware engineers, and software vendors to get the operating system ready, echoing CEO Steve Ballmer's call to make it simple, reliable and fast. To do that, Microsoft said it is collecting performance telemetry and application compatibility data, as well as information on usage.

"Think of all those Web sites, download pages, how-to-articles, training materials, and peripheral packages that need to be created -- this takes time, and knowing that the release candidate is the final code that we're all testing out in the open is reassuring for the ecosystem," Sinofsky said.

The release candidate will be the final Windows 7, since Microsoft plans to make it available to PC makers.

Once ready, the release candidate will be a refresher for the beta version. Users are supporting Microsoft's new course, telling the Windows 7 team to take its time and give users a quality product.

Microsoft is doing just that by not offering any release dates and saying the company will not be driven by "imposed deadlines." Sinofsky, however, did say that Microsoft is making progress and echoed Ballmer's promise to deliver the best release of Windows yet.

"Based on how the beta looks, it makes sense that the next version is considered a release candidate," said Michael Silver, vice president of research at Gartner. "The difference is in Microsoft's perception of how far along in development the product is. The quality of Windows 7 beta is probably better than Vista RC1."

"Then there can be multiple RCs, and there can be a month or more between RCs," Silver added.

Once Microsoft has completed its development process and fixed any glitches, Windows 7 will be preinstalled on new PCs and also be offered as a packaged product, according to Microsoft.

Western Digital today became the first manufacturer to announce the jump to 2TB in a single 3.5-inch hard disk drive. continues to solidify its role as a leader in the drive industry. The announcement marks a shift among hard disk manufacturers: WD is not normally known for being at the forefront of capacity jumps (typically Seagate is first to market with new capacities, including the previous capacity high-point, the Barracuda 7200.11 1.5TB drive.

But no word from Seagate on when it might offer a 2TB model. The company is currently drowning in issues with its flagship Barracuda 7200.11 series; drives in that series are reportedly having self-bricking issues.

The drive packs four 500GB platters, with 400 gigabits per square inch areal density. The drive is also part of WD's Green Power line of hard disk drives.

This line of drives first shipped a year ago, and was the first to actively bill themselves as environmentally friendly drives due to lower power consumption. The 2TB drive has several WD technologies inside that enable its combination of capacity and power performance. StableTrac reduces vibration by securing the motor shaft at both ends, which in turn allows for accurate head tracking during read and write operations; IntelliPower, which WD says adjusts the balance of spin speed, transfer rate and caching algorithms for optimal balance between performance and power consumption; IntelliSeek, which optimizes seek speeds to enable lower power consumption, noise, and vibration; and WD's NoTouch ramp load technology, which keeps the recording head from touching the disk media.

WD notes that, according to market research firm Trend Focus, over 10 percent of the 3.5-inch hard drive market is already at 1TB or higher.

### Microsoft IE8 Hits RC1 Milestone, Stops Clickjacking

On Monday, Microsoft's next-generation Web browser emerged out of the beta phase, with the announcement of Windows Internet Explorer 8 Release Candidate 1.

The release candidate is feature-complete, and its arrival means that the new browser will shortly be generally available. Microsoft is giving no concrete timetable for the final release; according to Microsoft senior product manager James Pratt, the release schedule will only be divulged when developer and tester feedback warranted it.

\*Check out our review of Internet Explorer 8 for full details on its features and performance.

The release candidate software comes in versions for Vista in 32-bit and 64-bit editions, as well as a 32-bit Windows XP edition. There's no installer for Windows 7, ironically, as Internet Explorer 8 will be the browser that ships with that new operating system.

Internet Explorer 8, while not drastically different in appearance from IE7, offers a revamped rendering engine, browsing aids, and security features. The RC1 version is only slightly different from the Beta 2 version, with the most important changes coming to its InPrivate

Browsing feature, which garnered considerable press attention at its first appearance. The feature has now been separated from another privacy feature, formerly called InPrivate Blocking, and now referred to as InPrivate Filtering.

This InPrivate Filtering addition prevents third-party Web content providers from gathering information about users' browsing habits from other sites they provide content to. InPrivate Browsing, on the other hand, prevents those with physical access to a PC from seeing where that other PC's users have been on the Web, by not saving browsing history, cookies, or cached pages.

IE8 will differ from IE7 by better conforming to open Web standards, but the new browser also includes a Compatibility Mode for sites that expect IE7's page rendering characteristics. With RC1, users will now be able to opt in to a list of sites compiled by Microsoft that require the mode, so they won't have to explicitly make the choice. The browser also improves on speed, particularly in startup time, though it still trails Google's Chrome and Mozilla's Firefox in JavaScript rendering speed. According to Microsoft's Pratt, however, JavaScript only makes up 20 percent of Web activity, and that the development team concentrated on other components that more noticeably affect how quickly pages load.

New browsing helpers include a Firefox-like address bar, which suggests sites you're trying to access based on your history and favorites. It also brings two helpers not found in any other browser: WebSlices and Accelerators. WebSlices give users a way to keep updated about a particular item on a web page, such as an eBay item being bid on. Accelerators let users access Web services such as maps, or translations for highlighted text, in a small window that doesn't require leaving the page.

Microsoft has also beefed up the browser's reliability by running in several processes, so that when a site in one tab crashes it need not bring down the whole browsing session, one of the notable features of the Google Chrome browser. IE8 uses color-coded tabs for related sites, though they can't be dragged out to the desktop to create new windows as they can in Chrome.

RC1 also includes protection against "Clickjacking," a ploy to get users to click on account buttons while covering the actual site being clicked on using a frame; the first browser available to counter this type of threat, Pratt said. The IE8 beta already includes a SmartScreen Filter, which not only blocks phishing sites, but sites known to distribute malware.

The news of the new browser launch comes as Microsoft finds itself under attack by the European Union for including a Web browser with its Windows operating system. Meanwhile Internet Explorer has been steadily losing market share to Firefox, with that browser recently passing the 20 percent mark.

You can download and try out the new browser at [www.microsoft.com/ie8](http://www.microsoft.com/ie8).

## ICANN Ponders Ways to Stop Scammy Web Sites

The overseer of the Internet's addressing system is soliciting ideas

for how to fix a problem that is enabling spammers and fraudulent Web sites to flourish.

The Internet Corporation for Assigned Names and Numbers (ICANN) has issued an initial report on fast flux, a technique that allows a Web site's domain name to resolve to multiple IP (Internet protocol) addresses.

Fast flux allows an administrator to quickly point a domain name to a new IP address, for example if the server at the first address fails or comes under a denial-of-service attack. It is legitimately used by content distribution networks such as Akamai to balance loads, improving performance and lowering data transmission costs.

But the technique has also been embraced by hackers and cybercriminals, who use it to make it harder for ISPs (Internet service providers) and law enforcement officials to close down phishing Web sites and other sites illegally hawking goods such as pharmaceuticals.

"Those engaged in these activities can frustrate the efforts of investigators to locate and shut down their operations by using fast-flux service networks to rapidly and continuously change the topology of the network on which their content is hosted," according to the report.

The main aim of cybercriminals is to keep their fraudulent Web sites up and running longer. Fast flux "is not an attack itself - it is a way for an attacker to avoid detection and frustrate the response to the attack," the report said.

That's done in part by modifying how long name servers around the Internet cache the IP address corresponding to the domain name. When a person visits a Web site, a local name server caches the IP address of the domain name. How long the local name server refers to its cached record for a Web site is controlled by the "time-to-live" setting in the official DNS (Domain Name System) record for a site, set by Web site's operator.

While "time-to-live" is typically set to hours or even days, a Web site's IP address can be change as often as every few minutes, redirecting to countless servers belonging to different ISPs, all of which would have to be taken down. In combination with the use of proxy servers and redirect commands, antiphishing efforts can turn into endless game of chase.

Consumers can be defrauded, as cybercriminals try to hack into Web hosting accounts in order to set up new nodes on their fast-flux networks, the report said.

The security community is faced with the challenge of trying to mitigate criminal use of fast flux but also not inadvertently restricting its legitimate uses.

One solution is quicker identification and shut down of domain names identified with abusive activity. Domain names could be revoked by a registrar, which in most cases would stop the site from working. Another solution would be to limit the ability of a registrant to repeatedly change name servers or eliminate automated name-server hopping, the report said.

The 121-page report, written by ICANN's Generic Names Supporting Organization (GNSO) lays out a series of other methods that could be used to mitigate the problem. GNSO will accept comments for 20 days and then do a final redraft of the report.

### Click Fraud Closed 2008 at All-Time High

Thanks in part to armies of compromised computers, click fraud reached an all-time high in the fourth quarter.

Click fraud lets Web sites increase revenue from ads supplied by services such as Google's AdSense or the Yahoo Publisher Network, though those companies take measures to screen out bogus links so advertisers don't have to pay. But that doesn't stop people from trying, according to a new report from Click Forensics, a company that monitors for click fraud and sells detection services.

"The overall industry average click fraud rate grew to 17.1 percent for the fourth quarter of 2008. That's up from 16.0 percent in the third quarter of 2008 and from the 16.6 percent rate reported for the fourth quarter of 2007," the company said Wednesday.

Humans can click on ads, but increasingly fraudsters turn to botnets, the swarms of computers taken over through remote attacks that can do fraudsters' bidding without computer users' knowledge.

"Traffic from botnets was responsible for 31.4 percent of all click fraud traffic in the fourth quarter of 2008. That's up from the 27.6 percent rate reported for the third quarter of 2008 and the 22.0 percent rate reported for the fourth quarter of 2007," Click Forensics said.

### After McColo Takedown, Spam Surges Again

Spammers have regrouped and are finding ways to send more junk mail despite recent efforts by security experts.

Spam levels dropped by almost half when rogue ISP (Internet service provider) McColo was taken offline in November. But some new botnets and even older ones are churning out more spam.

"At the current rates, we'll be back at those pre-McColo takedown levels probably within the next three to five weeks," said Adam Swidler, senior product marketing manager for Google Message Security, also known as Postini.

Google said Monday it has seen a 156 percent increase in spam since McColo went offline. McColo hosted the so-called command-and-control servers for botnets that are used to instruct PCs to send spam. The botnets included Rustock, Srizbi, Pushdo/Cutwail, Mega-D and Ghag.

McColo's takedown for the most part killed off the Srizbi botnet, which was blamed for sending a large proportion of the world's spam. But other botnets - which are essentially legions of hacked computers configured to send spam - are picking up the slack.

Mega-D, also known as Ozdok, is comprised of at least 660,000 PCs, according to MessageLabs, an e-mail security outfit now owned by Symantec. On average, PCs infected with Mega-D send out an astounding 589,402 messages per day, or around 409 per minute. All told, Mega-D is sending out 38 billion messages per day.

According to MessageLabs' latest figures released Monday, 74.6 percent of all e-mail was spam this month, a 4.9 percent increase over December. Percentages of spam can vary by vendor depending on the pool of PCs using their services, which are used to collect statistics on spam.

"We've seen a steady increase over the last two months," said Paul Wood, MessageLabs Intelligence Analyst with Symantec.

MessageLabs saw spam drop to around 58 percent of all e-mail when McColo went down, but rising to around 69 percent in December, Wood said.

Spammers are also changing their tactics to ensure their messages are not blocked, said Richard Cox, CIO for the antis spam organization Spamhaus.

When a computer is infected with code used to send spam, it sets up a mail server on the PC, which proceeds to pump out spam directly onto the Internet. But if that computer is noticed sending spam, it is added to a block list address ranges that shouldn't be sending unauthenticated mail.

As an alternative, spammers are using programs that detect a person's ISP and then route the mail through that ISP, which avoids it getting blocked when it is checked against the list, Cox said. The spam could be blocked, however, through other detection methods and analysis at a later point.

ISPs are "not really set up for" stopping that kind of abuse as of yet, Cox said. Further, many ISPs do not have security staff available constantly to act quickly when abuse is reported, he said.

Spamhaus is in the process of tracking which ISPs are hosting the command-and-control servers for some of the current flagrant botnets. Cox said he could not release more information.

McColo's shutdown came after a report appeared in the Washington Post in combination with pressure from computer security analysts. Although McColo was linked to Web sites hosting child pornography, it was the community of researchers rather than law enforcement that caused McColo's upstream providers to disconnect it from the Internet. Although McColo's servers were in the U.S., the people believed to run the operation were likely overseas.

#### Security Firm Sees Alarming Rise in 'Transient' Threats

Anti-virus firm AVG Technologies says an alarming rise in the number of virus-laden sites that are here today and gone tomorrow is causing security experts to re-think traditional virus protection strategies.

AVG reports the number of websites set up to steal your data has nearly doubled from about 150,000 per day to 300,000 since October 2008. More alarming to AVG is the fact those sites are short lived and vanish

sometimes within 24 hours. These "transient threats" make maintaining lists of dangerous websites extremely hard to manage, says Roger Thompson, chief research officer for AVG.

"Security firms can no longer rely on just blacklisting sites," Thompson says. AVG, like many other anti-virus companies, keeps track of rogue sites and updates its desktop anti-virus software with that list. But as the churn of new threats increases at an alarming rate blacklist databases become increasingly less effective.

AVG says protection of computers must now more heavily rely on identifying threatening behavior of a site. This method of protection relies on identifying when a site is attempting to attack your PC and stopping that attack before it happens.

AVG says that 60 percent of dangerous transient sites are up for one day and gone the next. One year ago rogue sites would stay alive on average 30 days giving security experts a chance to blacklist the site and identify the virus signature so it could create a defense against the virus and blacklist the site.

The majority of the threats presented by these sites are what is called a drive-by downloads. Meaning all you have to do is visit the site and malicious code can infect your computer. We've seen this before when a number of well-known sites discovered they had malware embedded in banner ads from third-party ad providers.

Here is more data that comes from AVG released today as part of a report "Transience, Stealth the Hallmarks of Today's Web Threats.".

- \* 94 percent of sites distributing 'fake codec' attacks - when the user is offered a codec, or video conversion tool, in order to view or download a particular video but is in reality a piece of malware - are usually active for less than 10 days, with 62 percent active for less than one day.

- \* 91 percent of sites distributing attacks from China -frequently stealing seemingly-harmless items like World of Warcraft game passwords which can be resold on sites like eBay for real money- are typically active for less than 12 days, with almost 50 percent active for less than one day.

- \* 72 percent of sites distributing fake anti-spyware products that in fact deposit spyware onto the user's machine and then offer to remove it for a fee are active on average for less than two weeks, with 28 percent active for less than one day

According to AVG, social networking sites are prime breeding grounds for these types of transient attacks. Social networking users are more trusting and less suspicious in these environments making them more likely to click on links that will take them onto the mean streets of the World Wide Web. That's not particularly surprising, especially considering recent news about the conficker worm as well as malicious attacks found lurking on President Barack Obama's campaign website.

Unsurprisingly, AVG suggests that its products are ideal to combat transient threats. AVG's current free and fee desktop anti-virus products scan how a website is behaving to determine whether or not it contains malware as opposed to looking for specific, known viruses or restricting access based on blacklist. Competing anti-virus firms also

offer similar two-prong approaches (blacklist and real-time protection) in protecting your desktop. For a list of free and fee anti-virus protection check out PC World's Downloads.

Along with anti-virus software there are many other things you can do to reduce threats to your computer. PC World contributor Andrew Brandt outlines many of them in his report 17 high-risk security threats and how to fix them.

### Another Trojan Horse Stalks Mac Software Pirates

In less than a week, two different forms of Trojan horses have invaded Macs whose users downloaded pirated copies of first Apple iWork 09 and now Adobe Photoshop CS4.

As of Monday morning, 21,000 people had downloaded the first Trojan horse in a pirated copy of iWork, according to Intego, a UK-based developer of privacy and security software for the Mac. The second Trojan horse in a pirated copy of Photoshop had been downloaded 5,000 times.

"If we extrapolate the total number, it is twice that," said Peter James, a spokesperson for Intego. The company is warning Mac users to avoid downloading pirated software.

Security analyst Jose Nazario of Arbor Networks advised, "Pay for your software. It is not antivirus, it is not patch. There is no vulnerability other than your gullibility."

The Photoshop exploit, OSX.Trojan.iServices.B Trojan Horse, considered a serious threat, is found in pirated software distributed through BitTorrent trackers and other sites with links to pirated software. The virus is bundled with copies of Adobe Photoshop CS4 for Macs through an application that serializes the program.

Users who download the pirated software will first run a crack application that installs a backdoor director. Once installed, the malware sends an alert to the creator, which can then connect to the infected Mac and take control.

Because the Trojan horse creates a new attack with a different name, it's more difficult to remove.

"The software installed could do a whole lot of stuff and can be downloading new or totally different software, and leaves open the possibility of keystroke loggers," James said.

"Basically it forces computers to join a peer-to-peer botnet," Nazario said. "If they want to install DDOS agent, which is one of the things they can do with a botnet - they can do that."

And they have, according to James, who said his company has watched computers actively participating in DOS attacks.

Nazario said the motivation behind the attacks is hard to read. "I don't think it is necessarily targeting pirates; rather, it is more of proof of concept on the Mac," he said. "It is someone exploiting the Mac."

James has his own theory. "People out there in the malware industry are realizing that by not targeting the [Mac] market, they are missing out on an incredibly large market share," James said. "Mac people have been in the minority for some time and the Apple market share is growing quarter to quarter."

Malware coders may also realize that the Windows market is increasingly difficult to penetrate, according to James.

"Mac users have been complacent and don't have the reflex that Windows users have," he said. "People behind malware realize the Mac users are not security savvy."

=~::~~==

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: [dpj@atarinews.org](mailto:dpj@atarinews.org)

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.